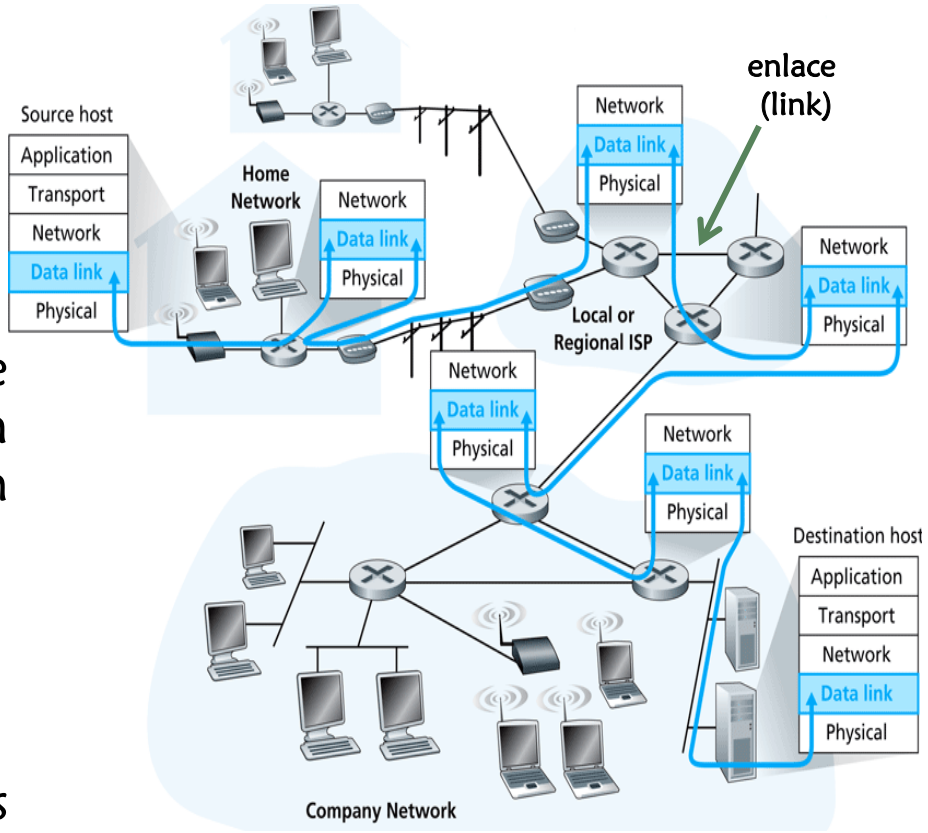
Capítulo 5

Capa de Enlace de Datos

Introducción

Algo de terminología:

- nodos → hosts y enrutadores.
- enlaces → Canales de comunicación que conectan nodos adyacentes a lo largo de un camino de comunicación.
  - Enlaces cableados
  - Enlaces inalámbricos
  - LANs
- La unidad de datos de capa 2 es una trama(frame), encapsula un datagrama.



La Capa de enlace de datos tiene la responsabilidad de transferir datagramas desde un nodo al nodo adyacente a través de un enlace.

- Los datagramas son transferidos por diferentes protocolos de enlace en diferentes enlaces:
  - Ethernet (primer enlace), Frame Relay (enlaces intermedios), 802.11 (último enlace).
- Cada protocolo de enlace provee diferentes servicios
  - puede o no proveer transferencia confiable sobre el enlace.

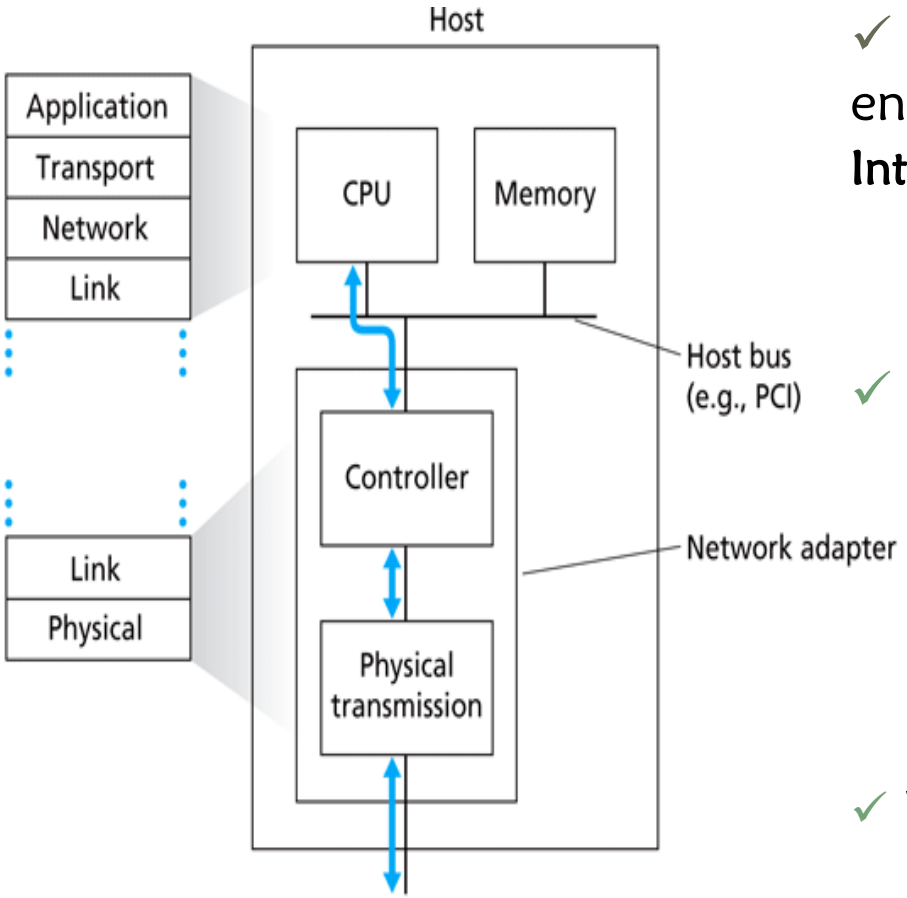
Servicios de Capa Enlace

- **Construcción de tramas** (*framing*) (Servicio Básico)
  - Se encapsula el datagrama en una trama.
    - Se agregan encabezados.
  - La estructura de la trama es especificada por el protocolo de la capa de enlace.

- **Acceso al medio** (*link acces*) (Servicio Básico)
  - MAC (medium access control), especifica las reglas de cómo transmitir las tramas sobre el enlace.
  - Acceso al medio si se trata de un acceso compartido.
  - Dirección "MAC" usada en encabezados de tramas para identificar fuente y destino.
    - Diferente de dirección IP!

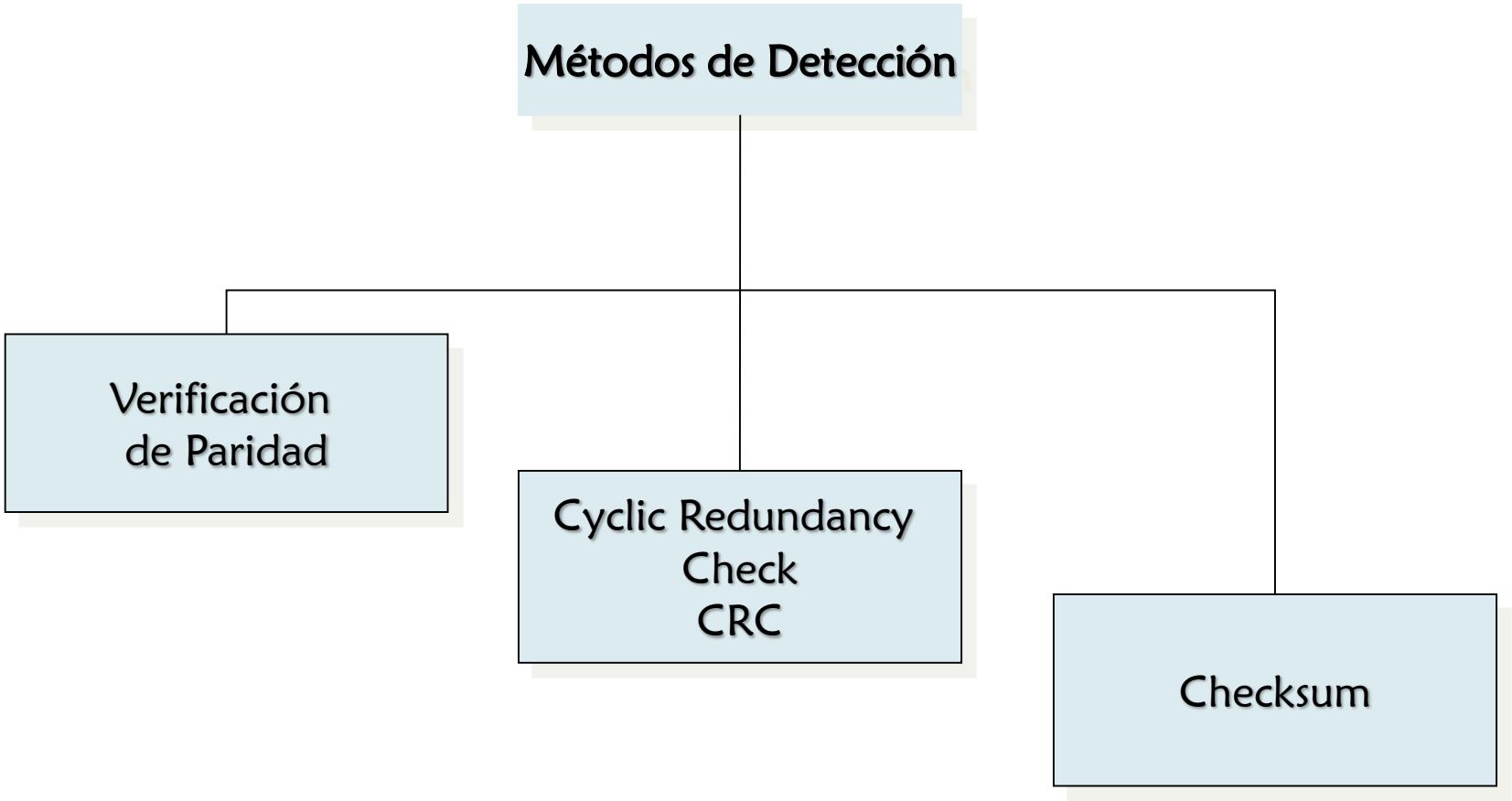
- **Entrega confiable entre nodos adyacentes**
  - Garantizar que los datagramas atraviesen el enlace sin error.
- **Control de Flujo**
  - Cada lado del enlace tiene un límite de almacenamiento.
- **Detección de Errores**
  - Errores causados por atenuación de señal y ruido.
  - Receptor detecta presencia de errores:
    - Pide al transmisor retransmisión o descartar la trama.
- **Corrección de Errores**
  - Receptor identifica *y corrige* error(es) de bit(s) sin solicitar retransmisión.
- **Half-duplex and full-duplex**
  - full duplex → los nodos de ambos extremos pueden transmitir al mismo tiempo.

Adaptadores de comunicación

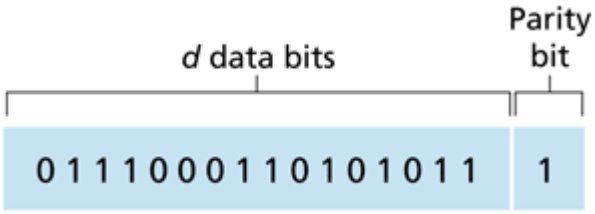


- ✓ La capa de enlace es implementada en un "adaptador" (**NIC**, **Network Interface Card**).
  - ✓ Tarjetas Ethernet, PCMCI, ó 802.11.
- ✓ Lado transmisor:
  - ✓ Encapsula el datagrama en una trama.
  - ✓ Agrega bits de verificación de errores, control de flujo, etc.
- ✓ Lado receptor:
  - ✓ Extrae datagrama y lo pasa al nodo receptor.

Métodos de Detección



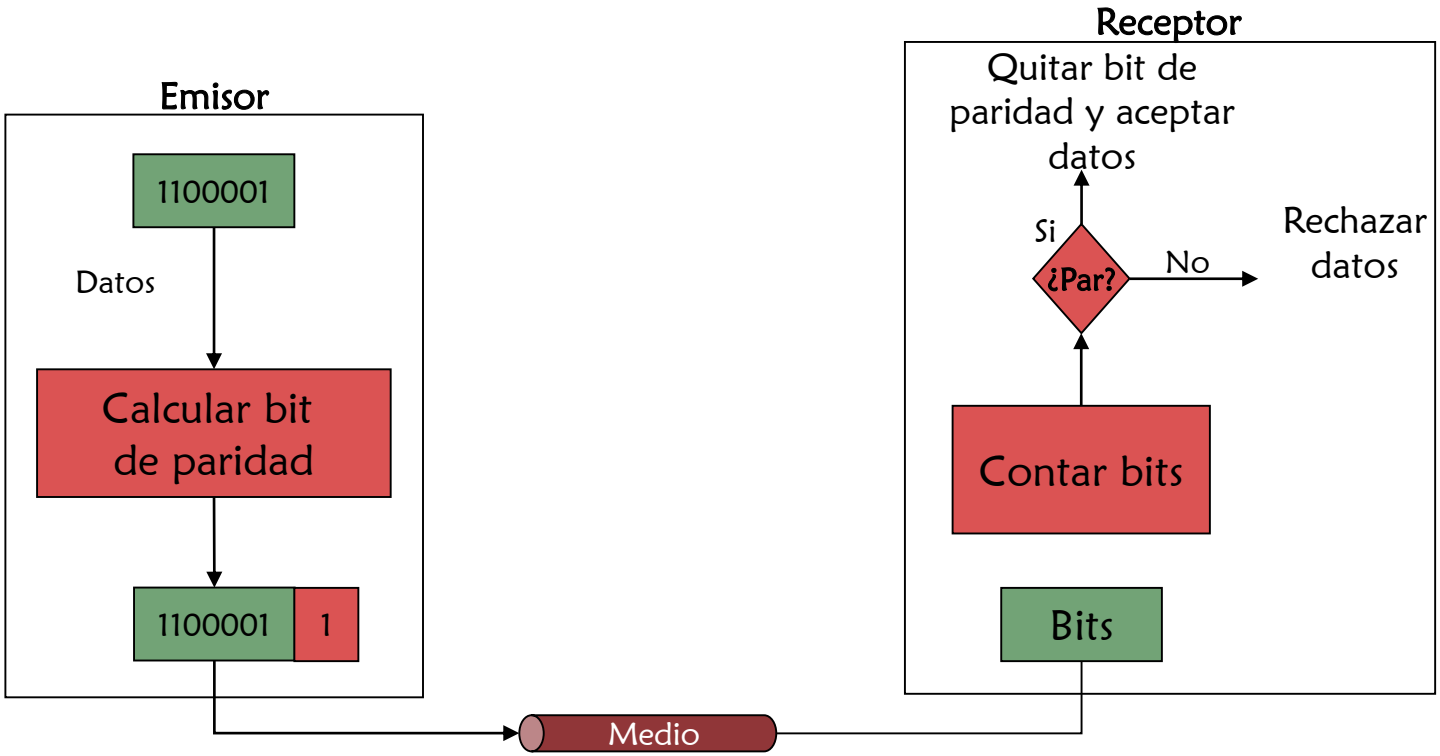
Verificación de paridad



✓ Bit de Paridad Simple:

- Detecta errores simples

Un bit redundante, llamado **bit de paridad**, es añadido a las unidades de datos, de tal manera que el número de 1's en la unidad (incluyendo el bit de paridad) sea par.



Ejemplo

- Supongamos que el emisor desea enviar la palabra *world*. En ASCII:

  1110111 1101111 1110010 1101100 110010

- Se agrega un bit de paridad por letra:

  11101110 11011110 11100100 11011000 1100101

- Supongamos que el emisor recibe la información sin corrupción.
  - El receptor cuenta los 1s en cada carácter y obtiene números pares (6, 6, 4, 4, 4). Los datos son aceptados.
- Ahora supongamos que se recibe la siguiente información:

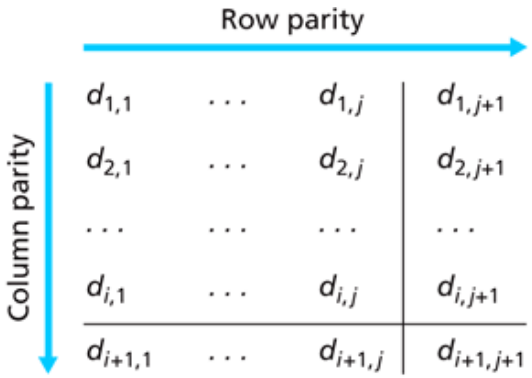
  11111110 11011110 11101100 11011000 11001001

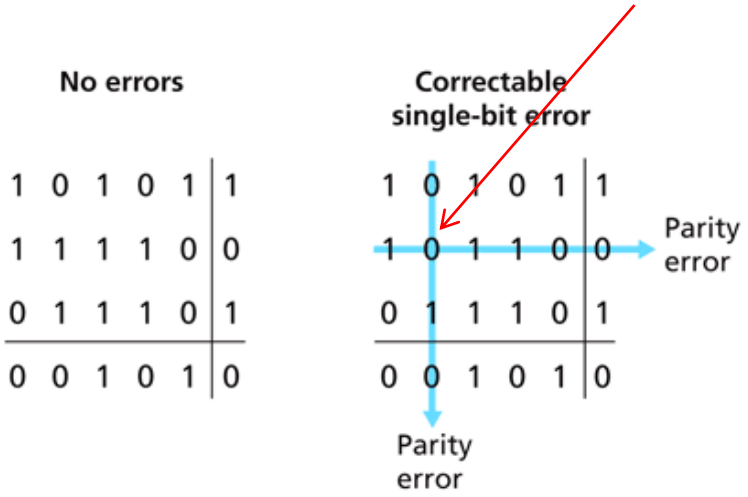
  - El receptor cuenta los 1s en cada carácter y obtiene números impares (7, 6, 5, 4, 4). Los datos son descartados y pide retransmisión.

✓ Bit de paridad de dos dimensiones:

- Detecta y *corrige* errores simples

Un bloque de bits es organizado en una tabla (renglones y columnas).

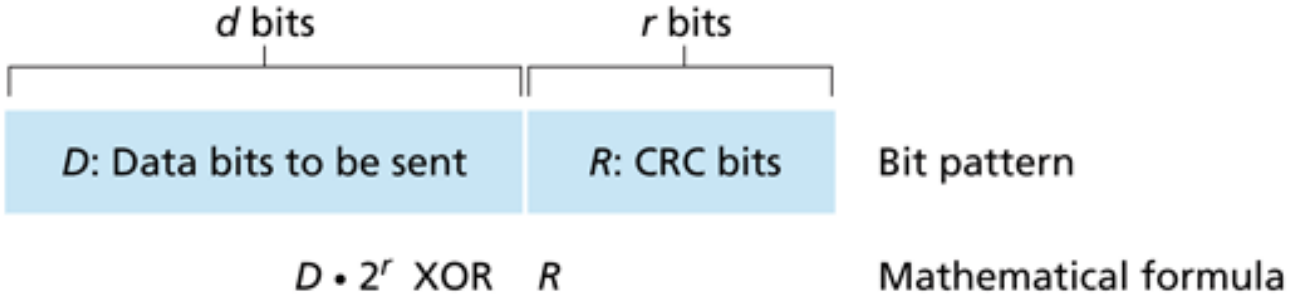




Verificación de Redundancia Cíclica

- CRC → Cyclic Redundancy Check.
- Estos códigos utilizan la aritmética modular para detectar una mayor cantidad de errores, se usan operaciones en módulo 2 y las sumas y restas se realizan sin acarreo (convirtiéndose en operaciones de tipo O-Exclusivo o XOR). Además, para facilitar los cálculos se trabaja, aunque sólo teóricamente, con polinomios.
- La finalidad de este método es crear una parte de redundancia la cual se añade al final del código a transmitir (como en los métodos de paridad) que siendo la más pequeña posible, detecte el mayor número de errores que sea posible.
- **El polinomio generador**: es un polinomio elegido previamente y que tiene como propiedad minimizar la redundancia. Suele tener una longitud de 16 bits, para mensajes de 128 bytes.
- Un ejemplo de polinomio generador usado normalmente en las redes WAN es:

$$g(x) = x^{16} + x^{12} + x^5 + 1$$



Ejemplo

- Datos:
  - Mensaje codificado en binario: 1101001
  - Polinomio generador: $x^4 + x + 1$

- Operaciones:
  - ✓ 1º Obtener el polinomio equivalente al mensaje: $x^6 + x^5 + x^3 + 1$
  - ✓ 2º Multiplicar el mensaje por x^4 (añadir 4 ceros por la derecha): $x^{10} + x^9 + x^7 + x^4$
  - ✓ 3º Dividir en binario el mensaje por el polinomio generador y sacar el resto: $x^2 + 1$
  - ✓ 4º sumar el mensaje con el residuo (en módulo 2 también): $x^{10} + x^9 + x^7 + x^4 + x^2 + 1$
  - ✓ 5º Transmitir el mensaje

- El equipo receptor debe comprobar el código CRC para detectar si se han producido o no errores.

Ejemplo de los cálculos del receptor:

1º Mediante el protocolo correspondiente acuerdan el polinomio generador

2º Divide el código recibido entre el polinomio generador

3º Comprueba el resto de dicha operación

3.1 Si el resto es cero, no se han producido errores

Procesar el mensaje

3.1 Si el resto es distinto de cero, significa que se han producido errores

Reenviar el mensaje

3.2 Intentar corregir los errores mediante los códigos correctores

Checksum

Objetivo: detectar "errores" (bits invertidos) en segmentos transmitidos.

Transmisor:

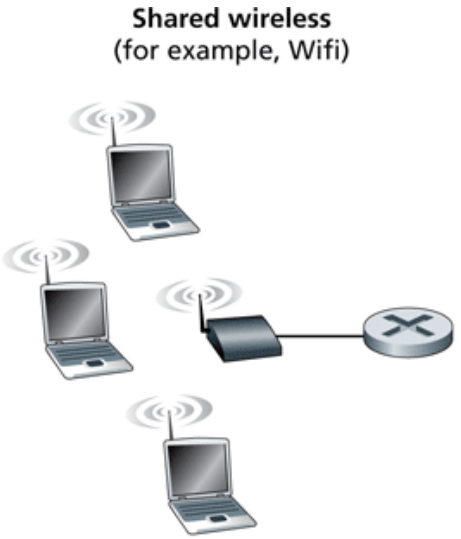
- Trata el contenido de los segmentos como una secuencia de enteros de 16 bits.
- checksum: suma del contenido del segmento (complemento 1 de la suma).
- Tx pone el valor del checksum en el campo correspondiente de UDP o TCP.

Receptor:

- Calcula el checksum del segmento recibido.
- Verifica si el checksum es igual al del campo recibido:
  - NO → error detectado.
  - SI → no hay error.

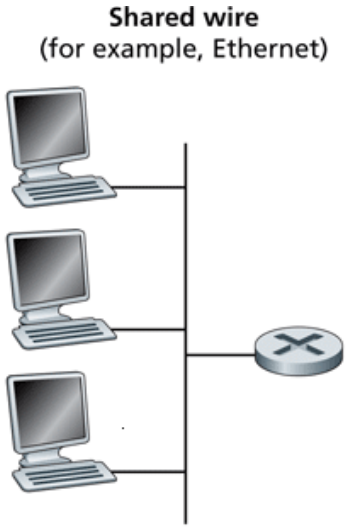
Protocolos de acceso múltiple

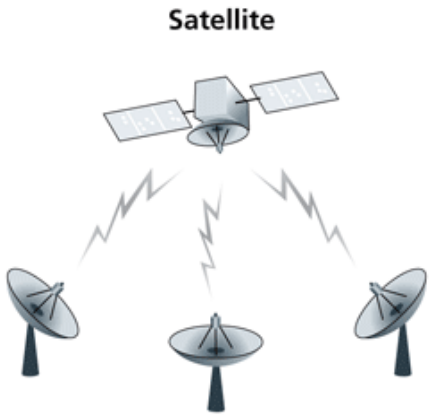
- Tipos de enlace de red
  - Enlaces punto a punto.
  - Enlaces broadcast.



- Principal problema

¿Cómo coordinar los accesos múltiples de envío y recepción cuando se comparte el canal de broadcast?





- Usan un canal simple de difusión compartida.
- Puede haber dos o más transmisiones simultáneas por nodos:
  - colisión → si un nodo recibe dos o más señales al mismo tiempo.

Protocolos de acceso múltiple

- Algoritmo distribuido que determinan cómo los nodos comparten el canal.
  - Determina cuándo un nodo puede transmitir.
- La comunicación para ponerse de acuerdo sobre cómo compartir debe usar el mismo canal!
  - no hay canal "fuera de banda" para coordinación.

Supongamos un canal broadcast de tasa R bps

1. Cuando un nodo quiere transmitir, este puede enviar a tasa R.
2. Cuando M nodos quieren transmitir, cada uno puede enviar en promedio una tasa R/M.
3. Completamente descentralizado:
   - No hay nodo especial para coordinar transmisiones.
   - No hay sincronización de reloj o ranuras.
4. Es simple.

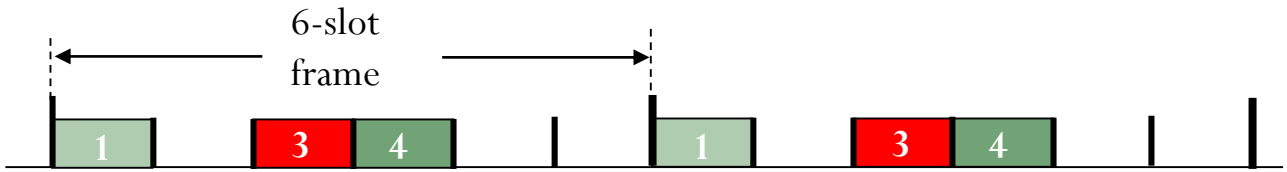
Categorías de los protocolos de acceso múltiple

- **Canal Subdividido ("particionado")** [channel partitioning protocols]
  - Divide el canal en pequeños "pedazos" (ranuras de tiempo, frecuencia, código).
  - Asigna pedazos a un nodo para su uso exclusivo.
- **Acceso Aleatorio** [random access protocols]
  - Canal no es dividido, permite colisiones.
  - Hay que "recuperarse" de las colisiones.
- **"Tomando turnos"** [taking-turns protocols]
  - Los nodos toman turnos, pero los nodos que envían más información pueden tomar turnos más largos.

Protocolos de Canal subdividido

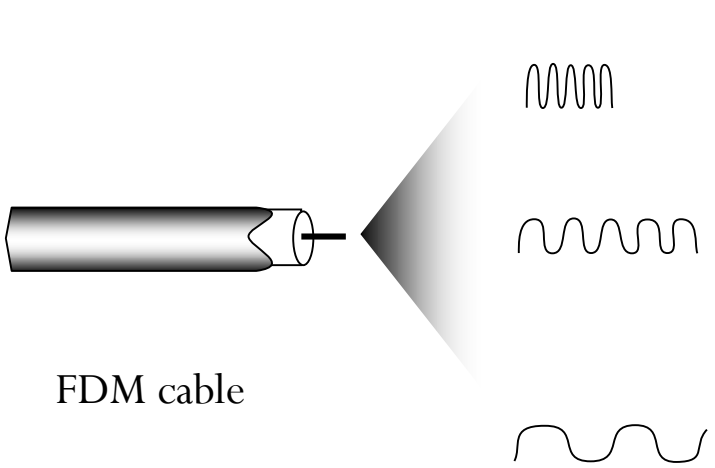
✓TDMA: Time Division Multiple Access

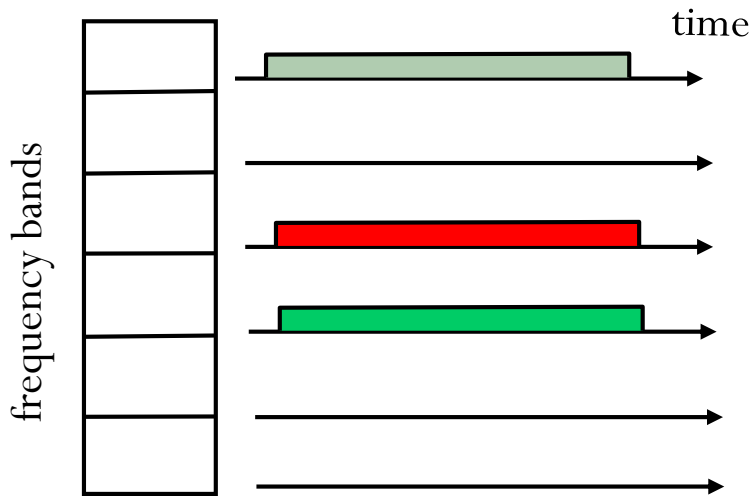
- Acceso a canales es en "rondas".
- Cada estación obtiene una ranura de largo fijo (largo= tiempo de transmisión del paquete) en cada ronda.
- Ranuras no usadas no se aprovechan.
- Ejemplo: LAN con 6 estaciones, 1,3,4 tienen paquetes, ranuras 2,5,6 no usadas.



✓FDMA: Frequency Division Multiple Access

- Espectro del canal es dividido en bandas de frecuencia.
- Cada estación obtiene una banda de frecuencia fija.
- Tiempo de transmisión no usado no es aprovechado.
- Ejemplo: LAN de 6 estaciones, 1,3,4 tiene paquetes, bandas de frecuencias 2,5,6 no se aprovechan.





✓CDMA: Code Division Multiple Access

- Asigna un diferente código a cada nodo.
- Cada nodo utiliza este código para enviar los bits.
- Si el código es elegido cuidadosamente, las redes CDMA tendrán la propiedad que diferentes códigos puedan transmitirse simultáneamente.
- Es utilizado en sistemas militares y en la telefonía celular.

Protocolos de Acceso Aleatorio

- Cuando un nodo tiene paquetes que enviar
  - Transmite a la tasa máxima del canal R.
  - No hay coordinación entre nodos.
- Si dos o más nodos transmiten se produce “colisión”.
- Especifican:
  - Cómo detectar colisiones.
  - Cómo recuperarse de una colisión (vía retransmisiones retardadas).
- Ejemplos de protocolos MAC de acceso aleatorio:
  - ALOHA ranurado.
  - ALOHA.
  - CSMA, CSMA/CD, CSMA/CA.

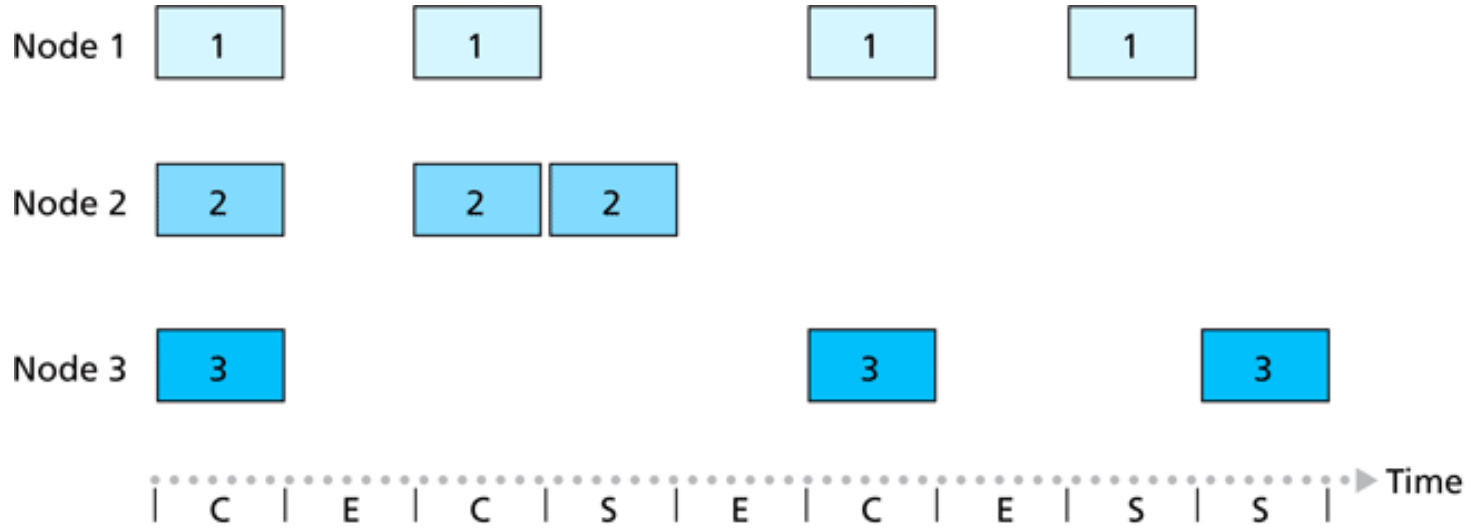
✓ALOHA ranurado

Suposiciones:

- Todas las tramas tienen igual tamaño.
- Tiempo es dividido en ranuras de igual tamaño. La ranura = tiempo para transmitir una trama.
- Nodos comienzan a transmitir tramas sólo al inicio de cada ranura.
- Nodos están sincronizados
- Si 2 o más tramas colisionan en una ranura, todos los nodos detectan la colisión.

Operación:

- Cuando el nodo tiene una nueva trama a enviar, la transmitirá completa en la siguiente ranura.
- Si no hay colisión, el nodo puede enviar una nueva trama en la siguiente ranura.
- Si hay colisión, el nodo retransmite la trama en cada ranura subsiguiente con probabilidad p hasta que la transmisión sea exitosa.



Ventajas:

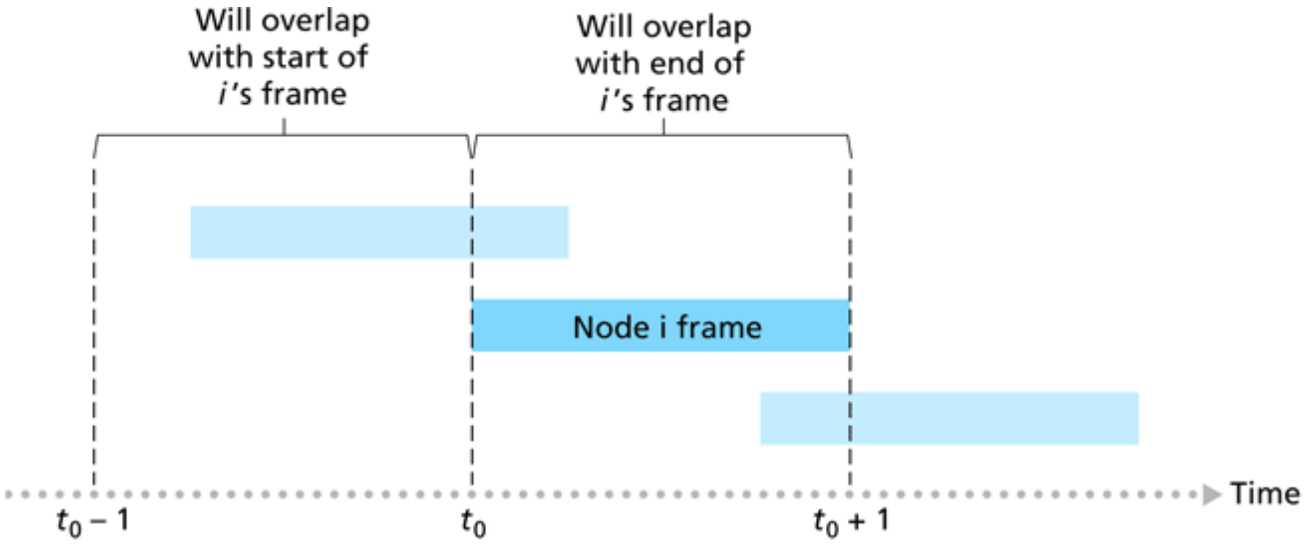
- Un único nodo activo puede transmitir continuamente a la tasa máxima del canal.
- Altamente descentralizado: cada nodo es independiente y decide cuando retransmitir.
- Protocolo simple.

Desventajas:

- Colisiones, ranuras desperdiciadas.
- Ranuras no ocupadas.
- En mejor caso se logra 37% de utilización.

✓ALOHA puro

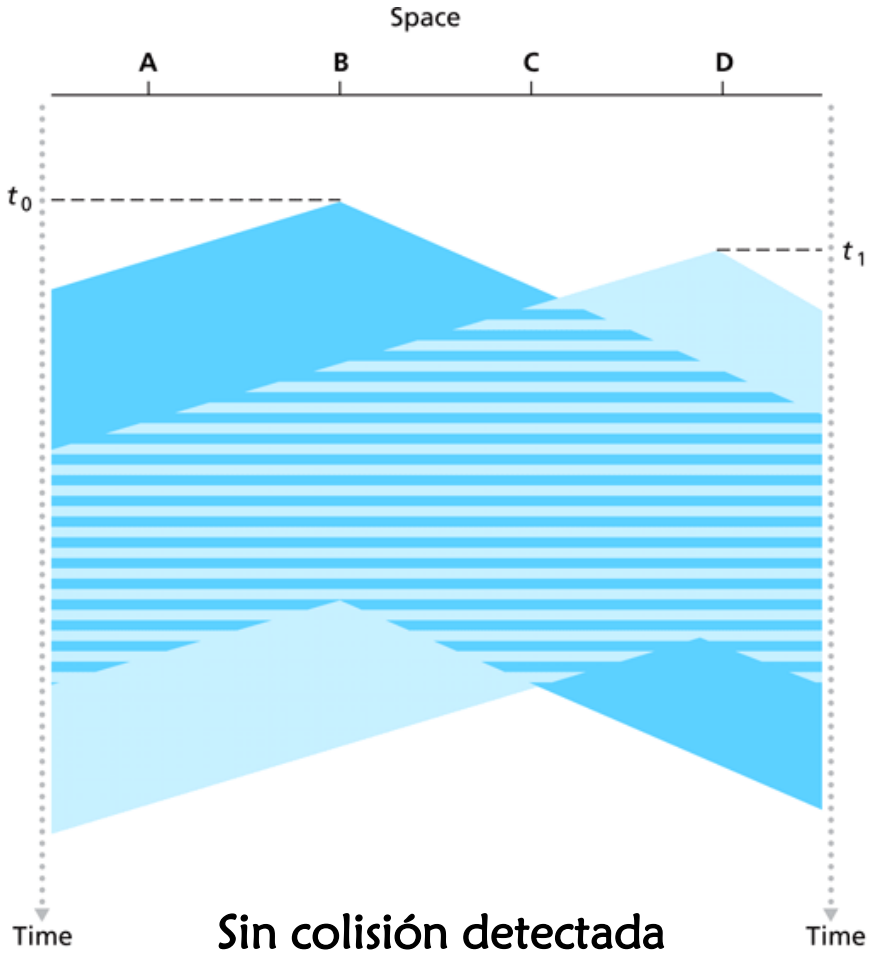
- Aloha no ranurado: más simple, no hay sincronización.
- Cuando una trama debe ser enviada
  - transmitir inmediatamente.
- Probabilidad de colisión aumenta:
  - Trama enviada a t_0 colisiona con otras tramas enviadas en $[t_0-1,t_0+1]$
- Probabilidad de éxito de transmisión de un nodo 18%.



✓CSMA (Carrier Sense Multiple Access)

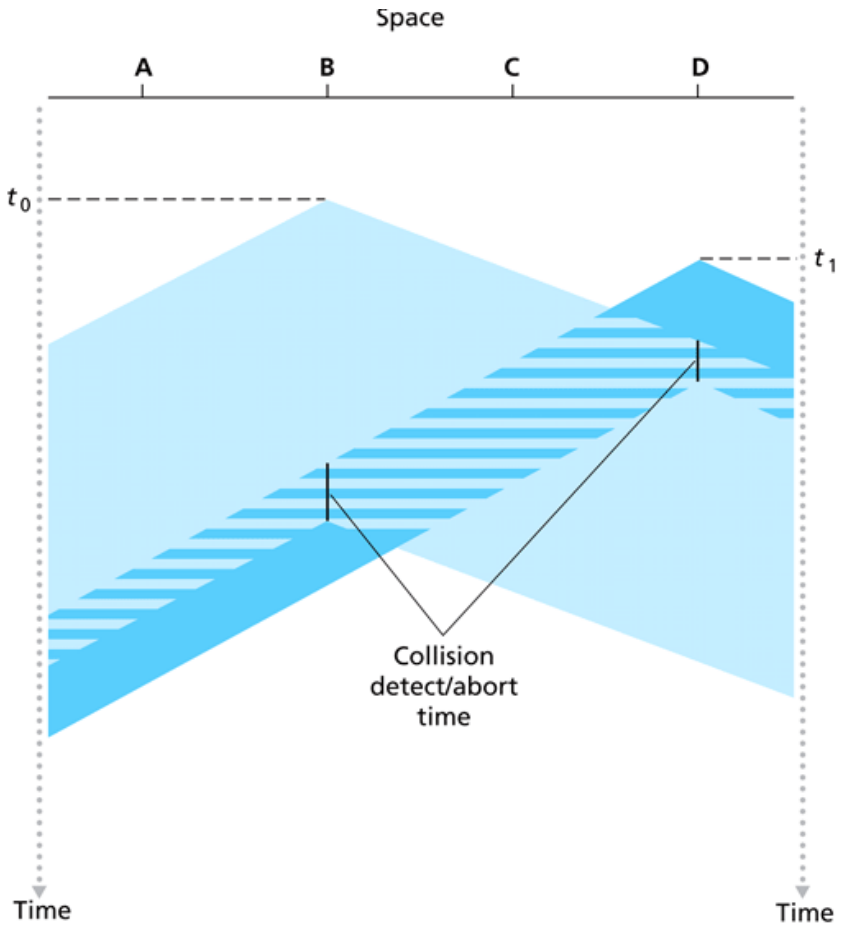
- sensar portadora antes de transmitir:
  - Si el canal está disponible, el nodo empieza la transmisión.
  - Si el canal está ocupado, el nodo espera (*"backs off"*) un tiempo aleatorio para volver a sensar el canal.

Colisiones en CSMA



Sin colisión detectada

Con colisión detectada



✓CSMA/CD (Detección de Colisiones)

- Carrier sensing, similar a CSMA:
  - colisiones son *detectadas* en corto tiempo.
  - transmisiones en colisión son abortadas, reduciendo el mal uso del canal.

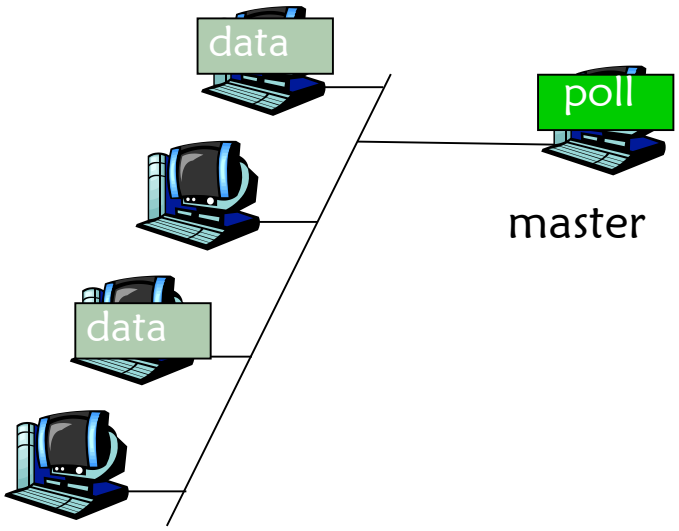
- Detección de colisiones:
  - Fácil en LANs cableadas: se mide la potencia de la señal, se compara señales transmitidas con recibidas.
  - Difícil LANs inalámbricas: receptor es apagado mientras se transmite.

Protocolos MAC de "toma de turnos"

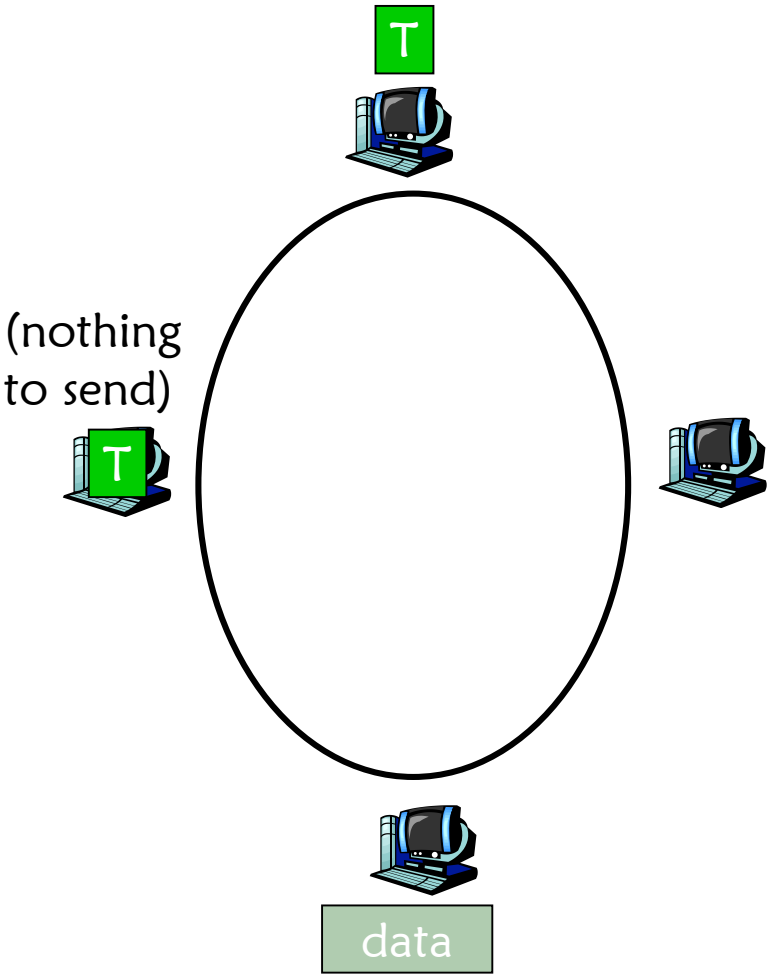
- Protocolos MAC que particionan el canal
  - Son eficientes en alta carga:
    - comparten el canal equitativamente.
  - Son ineficientes a baja carga:
    - hay retardo en acceso al canal, 1/N del ancho de banda es asignado aún si hay sólo un nodo activo!
- Protocolos de acceso aleatorio
  - Son eficientes a baja carga:
    - un único canal puede utilizar completamente el canal.
  - Son ineficiente en alta carga:
    - demasiadas por colisiones.
- Protocolos de "toma de turnos"
  - Buscan lo mejor de ambos protocolos!

✓ *Polling Protocol*

- Nodo maestro "invita" a nodos esclavos a transmitir en turnos.
- Desventajas:
  - Retardo.
  - Punto único de falla (maestro).



✓ Token-Passing Protocol



- **Token** (testimonio) de control es pasado de nodo en nodo secuencialmente.
- Hay un mensaje con el token.
- Desventajas:
  - Retardo.
  - Punto único de falla (el token).
- Ejemplos que utilizan este protocolo:
  - FDDI
  - IEEE 802.5 (Token Ring)

Resumen de protocolos MAC

¿Qué hacemos en un medio compartido?

- **Subdivisión del canal**
  - por tiempo, frecuencia, o código.
- **Subdivisión aleatoria (dinámica)**
  - ALOHA, ALOHA-R, CSMA, CSMA/CD.
  - CSMA/CD es usado en Ethernet.
  - CSMA/CA es usado en 802.11.
    - Sensado de portadora: fácil en algunas tecnologías (cable), difícil en otras (inalámbricas).
- **Toma de turnos**
  - *polling*, o *token-passing*

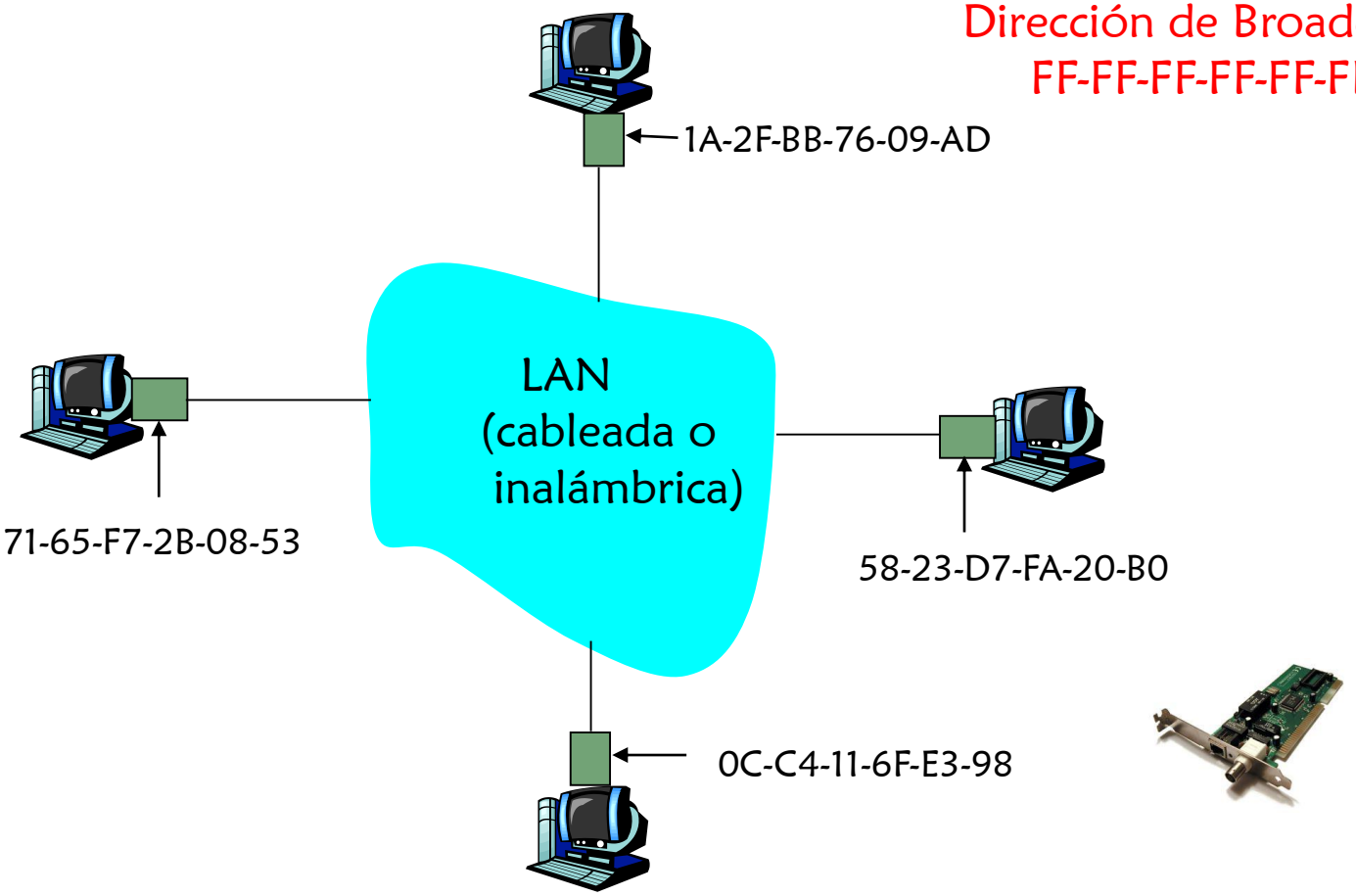
Direccionamiento MAC

- Direcciones IP son de 32-bit
  - Son direcciones de la capa de Red.
  - Son usadas para conducir un datagrama a la subred destino.
- Dirección MAC (o LAN o física o Ethernet)
  - Son usadas para conducir un datagrama a otra interfaz físicamente conectada en la misma red.
  - Son de 48 bits (en mayoría de LANs) están grabadas en una ROM de la tarjeta adaptadora.

Direccionamiento MAC

- Permite la distribución local de tramas en Ethernet.
- Cada computadora tiene una dirección física única.
- Se conoce con los siguientes nombres:
  - Dirección física que se ubica en la NIC
  - Dirección MAC
  - Dirección hardware
  - Dirección de la NIC
  - Dirección de la capa 2.
  - Dirección Ethernet.

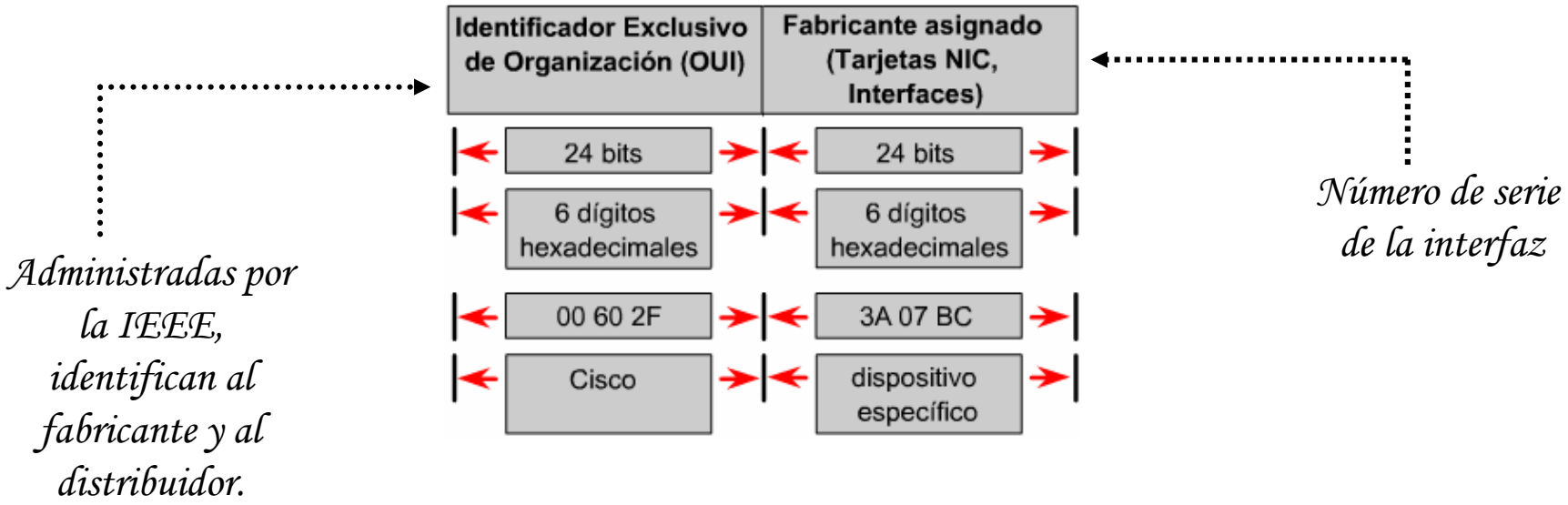
Cada adaptador de la LAN tiene una dirección única



Formato de la dirección MAC

- Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales.

- Las direcciones MAC, se denominan direcciones integradas (BIA, burned-in addres), se graban en (ROM) y se copian en (RAM) cuando se inicializa la NIC.



OUI list

00-0D-60 000D60	(hex) (base 16)	IBM Corporation 3039 Cornwallis Road Dept FCGA, Bldg 660, Office F106 Research Triangle Park NC 27709 UNITED STATES

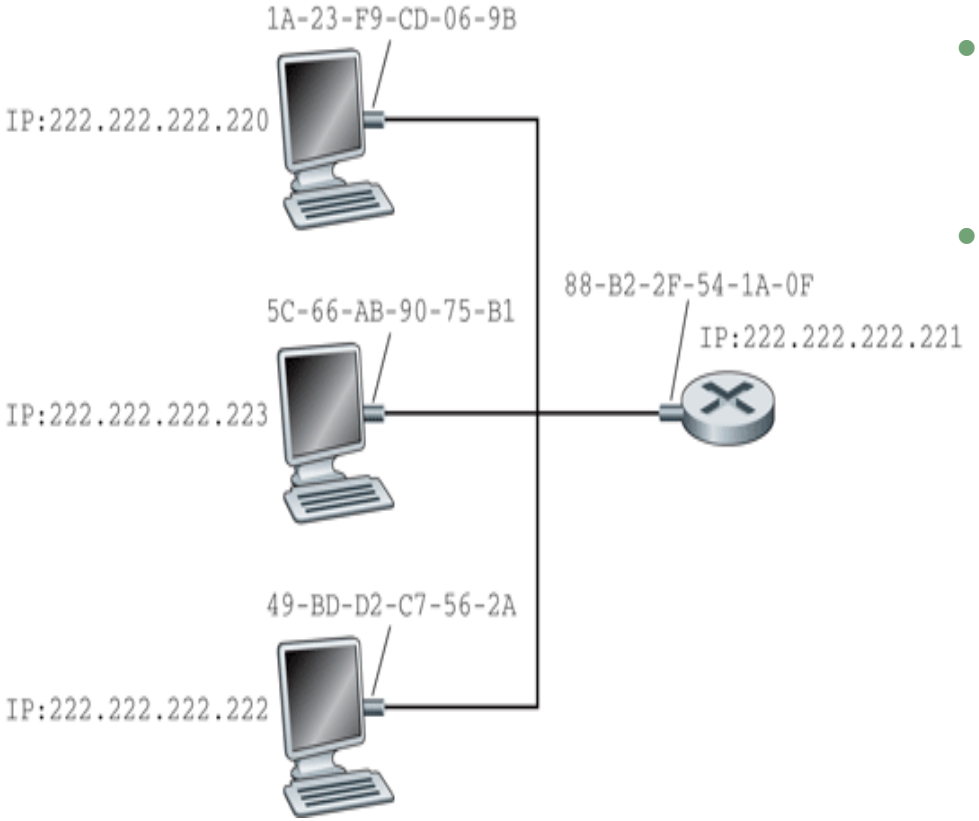
http://standards.ieee.org/regauth/oui/oui.txt

Utilidad de la MAC

- Sin la MAC, la LAN sería sólo un grupo de computadoras sin identificadores, y sería imposible enviar una trama Ethernet.
- Las LAN Ethernet y 802.3 son redes de difusión (broadcast), es decir, todas las estaciones ven todas las tramas.
- Cuando un dispositivo quiere enviar datos a otro dispositivo:
  - Se abre una ruta de comunicación hasta el otro dispositivo empleando su dirección MAC.
  - La NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección física de destino que lleva la trama de datos.
  - Si no existe coincidencia la NIC descarta la trama de datos.
  - Si hay coincidencia, la NIC hace una copia, saca los datos del envoltorio y los entrega a la computadora para que ésta los procese mediante los protocolos de capa superior como IP y TCP.

Protocolo de Resolución de Direcciones (ARP)

¿Cómo se determina la dirección MAC conociendo la dirección IP?



[RFC 826]

- Cada nodo IP (Host o Router) de la LAN tiene una tabla ARP.
- Tabla ARP: mapean direcciones IP/MAC para algunos nodos de la LAN:

  < IP address; MAC address; TTL >

  - TTL (Time To Live): tiempo de expiración para el mapeo (típicamente 20 min).

Operación ARP: Dentro de la misma LAN

- **A** quiere enviar un datagrama a **B**, y la dirección MAC de **B** no está en tabla ARP de **A**.
- **A** difunde (broadcasts) un paquete consulta (query) ARP, conteniendo la IP de **B**.
  - Dirección destino MAC =

    FF-FF-FF-FF-FF-FF
  - Todas las máquinas de la LAN reciben la consulta ARP.
- **B** recibe paquete ARP, y responde a **A** con su dirección MAC.
  - La respuesta es enviada a la MAC de **A** (unicast).
- **A** guarda (caché) el par IP-a-MAC en su tabla ARP hasta que la información envejece (times out).
  - La información expira a menos que sea actualizada.
- ARP es "plug-and-play":
  - Los nodos crean sus tablas de ARP sin intervención de la administradores.

IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Bibliografía

- *Computer Networking: A Top Down Approach*
  4th edition
  Jim Kurose, Keith Ross
  Addison-Wesley, July 2007, ISBN: 9780321497703

- *Network Fundamentals, CCNA Exploration Companion Guide*
  Mark A.Dye, Rick McDonald, Antoon W. Rufi
  Cisco Press, Noviembre 2007, ISBN: 9781587132087
  Capítulo 4